Teoría de la codificación

El espacio vectorial $\mathbb{Z}_2^n$

En el conjunto $\mathbb{Z}_2 = \{\bar{0},\bar{1}\}$ de las clases de los restos módulo 2, definimos las operaciones de suma y producto de clases (como se han definido en aritmética modular):

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

·	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

¿Cuál es el opuesto de $\bar{1}$ respecto de la suma? Pues $\bar{1}$, es decir, $-\bar{1}=\bar{1}$. Por tanto, en $\mathbb{Z}_2$, la RESTA se define igual que la suma: $\bar{0}-\bar{1}=\bar{0}+\bar{1}=\bar{1}-\bar{0}=\bar{1}+\bar{0}=\bar{1}$, $\bar{1}-\bar{1}=\bar{1}+\bar{1}=\bar{0}$, $\bar{0}-\bar{0}=\bar{0}$.

Con estas operaciones se verifica que $(\mathbb{Z}_2,+,\cdot)$ es un cuerpo conmutativo.

$\mathbb{Z}_2^n=\{(\bar{i}_1,\ldots,\bar{i}_n)/\ \bar{i}_k\in\mathbb{Z}_2=\{\bar{0},\bar{1}\},\ \forall k=1\ldots n\}$

Se define la suma $(\bar{i}_1,\ldots,\bar{i}_n)+(\bar{j}_1,\ldots,\bar{j}_n)=(\bar{i}_1+\bar{j}_1,\ldots,\bar{i}_n+\bar{j}_n)\in\mathbb{Z}_2^n$

Se define la ley externa $\bar{\lambda}\in\mathbb{Z}_2$, $\bar{\lambda}\cdot(\bar{i}_1,\ldots,\bar{i}_n)=(\bar{\lambda}\cdot\bar{i}_1,\ldots,\bar{\lambda}\cdot\bar{i}_n)\in\mathbb{Z}_2^n$

Ejemplos: $(\bar{1},\bar{1},\bar{0},\bar{1})+(\bar{0},\bar{1},\bar{0},\bar{0})=(\bar{1},\bar{0},\bar{0},\bar{1})=(\bar{1},\bar{1},\bar{0},\bar{1})-(\bar{0},\bar{1},\bar{0},\bar{0})$

$-\bar{1}\cdot(\bar{1},\bar{0},\bar{0},\bar{1})=\bar{1}\cdot(\bar{1},\bar{0},\bar{0},\bar{1})=(\bar{1},\bar{0},\bar{0},\bar{1})$

$\bar{0}\cdot(\bar{1},\bar{0},\bar{0},\bar{1})=(\bar{0},\bar{0},\bar{0},\bar{0})$

$(\bar{1},\bar{0},\bar{0},\bar{1})-(\bar{1},\bar{0},\bar{0},\bar{1})=(\bar{0},\bar{0},\bar{0},\bar{0})=(\bar{1},\bar{0},\bar{0},\bar{1})+(\bar{1},\bar{0},\bar{0},\bar{1})$

$(\mathbb{Z}_2^n,+,\cdot)$ es un espacio vectorial sobre $\mathbb{Z}_2$

Subespacios Vectoriales de $\mathbb{Z}_2^n$.

Ejemplos: $L(\{(\bar{0},\bar{0},\bar{0},\bar{0})\})=\{(\bar{0},\bar{0},\bar{0},\bar{0})\}$

$L(\{(\bar{1},\bar{0},\bar{0},\bar{1})\})=\{(\bar{1},\bar{0},\bar{0},\bar{1}),(\bar{0},\bar{0},\bar{0},\bar{0})\}$

$L(\{(\bar{1},\bar{0},\bar{0},\bar{1}),(\bar{1},\bar{0},\bar{0},\bar{0})\})=\{(\bar{0},\bar{0},\bar{0},\bar{0}),(\bar{1},\bar{0},\bar{0},\bar{1}),(\bar{1},\bar{0},\bar{0},\bar{0}),(\bar{0},\bar{0},\bar{0},\bar{1})\}$

(ya que $(\bar{0},\bar{0},\bar{0},\bar{1})=(\bar{1},\bar{0},\bar{0},\bar{1})+(\bar{1},\bar{0},\bar{0},\bar{0})$)

Dado $A=\{\vec{x}_1,\ldots,\vec{x}_k\}\subset\mathbb{Z}_2^n$ construimos:

$$L(A)=\{\bar{\lambda}_1\vec{x}_1+\ldots+\bar{\lambda}_k\vec{x}_k\ /\ \bar{\lambda}_1,\ldots,\bar{\lambda}_k\in\mathbb{Z}_2=\{\bar{0},\bar{1}\}\}$$

¿Cuántos vectores tiene L(A)? Si A son k vectores linealmente independiente, es decir, si A es base de L(A) (luego dim(L(A))=|A|=k), entonces $|L(A)|=2^k$ (es un buen ejercicio de combinatoria).

Ejemplo: $A=\{(\bar{1},\bar{0},\bar{0},\bar{1},\bar{0}),(\bar{1},\bar{0},\bar{0},\bar{0},\bar{1}),(\bar{1},\bar{0},\bar{0},\bar{0},\bar{0})\}$ ¿Son linealmente independientes?

$$\begin{pmatrix}\bar{1}&\bar{0}&\bar{0}&\bar{1}&\bar{0}\\ \bar{1}&\bar{0}&\bar{0}&\bar{0}&\bar{1}\\ \bar{1}&\bar{0}&\bar{0}&\bar{0}&\bar{0}\end{pmatrix}\xrightarrow[F_3-F_1]{F_2-F_1}\begin{pmatrix}\bar{1}&\bar{0}&\bar{0}&\bar{1}&\bar{0}\\ \bar{0}&\bar{0}&\bar{0}&\bar{1}&\bar{1}\\ \bar{0}&\bar{0}&\bar{0}&\bar{1}&\bar{0}\end{pmatrix}\xrightarrow{F_3-F_2}\begin{pmatrix}\bar{1}&\bar{0}&\bar{0}&\bar{1}&\bar{0}\\ \bar{0}&\bar{0}&\bar{0}&\bar{1}&\bar{1}\\ \bar{0}&\bar{0}&\bar{0}&\bar{0}&\bar{1}\end{pmatrix}(*)\xrightarrow{F_2-F_3}$$

(*) como la matriz tiene rango 3, los vectores son l.i. $\Rightarrow$ dim L(A)=3

$$\xrightarrow[F_2-F_3]{}\begin{pmatrix}\bar{1}&\bar{0}&\bar{0}&\bar{1}&\bar{0}\\ \bar{0}&\bar{0}&\bar{0}&\bar{1}&\bar{0}\\ \bar{0}&\bar{0}&\bar{0}&\bar{0}&\bar{1}\end{pmatrix}\xrightarrow[F_1-F_2]{}\begin{pmatrix}\bar{1}&\bar{0}&\bar{0}&\bar{0}&\bar{0}\\ \bar{0}&\bar{0}&\bar{0}&\bar{1}&\bar{0}\\ \bar{0}&\bar{0}&\bar{0}&\bar{0}&\bar{1}\end{pmatrix}$$ Forma canónica por filas (Echelon-Fila)

Por tanto, dim L(*A*)=3, |L(*A*)|=2^3=8,

$B_{L(A)}$= {($\bar{1},\bar{0},\bar{0},\bar{0},\bar{0}$), ($\bar{0},\bar{0},\bar{0},\bar{1},\bar{0}$), ($\bar{0},\bar{0},\bar{0},\bar{0},\bar{1}$)} es la base más sencilla de L(*A*).

Además, dim L(*A*)= rg(matriz que forman los vectores de *A*).

Base canónica o usual de $\mathbb{Z}_2^n$: {$\vec{e_1}$=($\bar{1},\bar{0},\ldots,\bar{0}$), $\vec{e_2}$=($\bar{0},\bar{1},\ldots,\bar{0}$),…,$\vec{e_n}$=($\bar{0},\ldots,\bar{0},\bar{1}$)}

Ecuaciones paramétricas e implícitas de un s.v. de $\mathbb{Z}_2^n$: evidentemente se construyen igual que para los subespacios vectoriales de $\mathbb{R}^n$. Veamos un ejemplo:

Sea el s.v. S=L({($\bar{1},\bar{1},\bar{1},\bar{0}$), ($\bar{1},\bar{0},\bar{0},\bar{1}$), ($\bar{1},\bar{1},\bar{1},\bar{1}$)}). Como estos tres vectores son s.g. de S y l.i. (se puede comprobar calculando el rango de la matriz que forman los tres vectores), se verifica que son base de S, por tanto dimS=3, |S|=2^3 y las ecuaciones paramétricas de S son:

Ecuaciones paramétricas de S: $\begin{pmatrix}\overline{x_1}\\ \overline{x_2}\\ \overline{x_3}\\ \overline{x_4}\end{pmatrix}=\bar{\alpha}\begin{pmatrix}\bar{1}\\ \bar{1}\\ \bar{1}\\ \bar{0}\end{pmatrix}+\bar{\beta}\begin{pmatrix}\bar{1}\\ \bar{0}\\ \bar{0}\\ \bar{1}\end{pmatrix}+\bar{\gamma}\begin{pmatrix}\bar{1}\\ \bar{1}\\ \bar{1}\\ \bar{1}\end{pmatrix}$ con $\bar{\alpha},\bar{\beta},\bar{\gamma}\in\mathbb{Z}_2\Rightarrow\begin{cases}\overline{x_1}=\bar{\alpha}+\bar{\beta}+\bar{\gamma}\\ \overline{x_2}=\bar{\alpha}+\bar{\gamma}\\ \overline{x_3}=\bar{\alpha}+\bar{\gamma}\\ \overline{x_4}=\bar{\beta}+\bar{\gamma}\end{cases}$

Se pueden calcular los 8 vectores de S dando valores $\bar{0}$ y $\bar{1}$ a los parámetros $\bar{\alpha},\bar{\beta}$ y $\bar{\gamma}$.

Eliminamos los parámetros $\bar{\alpha},\bar{\beta}$ y $\bar{\gamma}$ para obtener las ecuaciones implícitas de S:

Ecuaciones implícitas de S:

$$\left(\begin{array}{ccc|c}\bar{1}&\bar{1}&\bar{1}&\overline{x_1}\\ \bar{1}&\bar{0}&\bar{1}&\overline{x_2}\\ \bar{1}&\bar{0}&\bar{1}&\overline{x_3}\\ \bar{0}&\bar{1}&\bar{1}&\overline{x_4}\end{array}\right)\rightarrow\left(\begin{array}{ccc|c}\bar{1}&\bar{1}&\bar{1}&\overline{x_1}\\ \bar{0}&\bar{1}&\bar{1}&\overline{x_4}\\ \bar{1}&\bar{0}&\bar{1}&\overline{x_2}\\ \bar{0}&\bar{0}&\bar{0}&\overline{x_3}-\overline{x_2}\end{array}\right)\rightarrow\left(\begin{array}{ccc|c}\bar{1}&\bar{1}&\bar{1}&\overline{x_1}\\ \bar{0}&\bar{1}&\bar{1}&\overline{x_4}\\ \bar{0}&\bar{1}&\bar{0}&\overline{x_2}-\overline{x_1}\\ \bar{0}&\bar{0}&\bar{0}&\overline{x_3}-\overline{x_2}\end{array}\right)\rightarrow\left(\begin{array}{ccc|c}\bar{1}&\bar{1}&\bar{1}&\overline{x_1}\\ \bar{0}&\bar{1}&\bar{1}&\overline{x_4}\\ \bar{0}&\bar{0}&\bar{1}&\overline{x_2}-\overline{x_1}-\overline{x_4}\\ \bar{0}&\bar{0}&\bar{0}&\overline{x_3}-\overline{x_2}\end{array}\right)\Rightarrow$$

la ecuación implícita de S es: $\overline{x_3}-\overline{x_2}=\bar{0}$ ó $\overline{x_3}+\overline{x_2}=\bar{0}$.

Otro ejemplo: Sea S el s. v. de $\mathbb{Z}_2^3$ dado por las ecuaciones implícitas $\overline{x_1}+\overline{x_2}+\overline{x_3}=\bar{0}$.
Resolviendo este sistema obtenemos las ecuaciones paramétricas y la base de S.

$$\begin{cases}\overline{x_1}=-\bar{\alpha}-\bar{\beta}\\ \overline{x_2}=\bar{\beta}\\ \overline{x_3}=\bar{\alpha}\end{cases}\Rightarrow\begin{pmatrix}\overline{x_1}\\ \overline{x_2}\\ \overline{x_3}\end{pmatrix}=\bar{\alpha}\begin{pmatrix}\bar{1}\\ \bar{0}\\ \bar{1}\end{pmatrix}+\bar{\beta}\begin{pmatrix}\bar{1}\\ \bar{1}\\ \bar{0}\end{pmatrix}$$ Ecs. paramétricas de S y B_S={($\bar{1},\bar{0},\bar{1}$), ($\bar{1},\bar{1},\bar{0}$)}.

Así, dimS=2 y |S|=2^2. Por tanto, S={($\bar{0},\bar{0},\bar{0}$), ($\bar{1},\bar{0},\bar{1}$), ($\bar{1},\bar{1},\bar{0}$), ($\bar{0},\bar{1},\bar{1}$)}, siendo ($\bar{0},\bar{1},\bar{1}$) = ($\bar{1},\bar{0},\bar{1}$) + ($\bar{1},\bar{1},\bar{0}$).

Luego, si S es un s.v. de $\mathbb{Z}_2^n$ dado por sus ecuaciones implícitas, se verifica que

dimS=n – rg(matriz de coeficientes de sus ecs. implícitas).

Código Lineal de longitud n: es cualquier subespacio vectorial de $\mathbb{Z}_2^n$.

Ejemplo: Sea la matriz $H=\begin{pmatrix}\bar{0}&\bar{0}&\bar{0}&\bar{1}&\bar{1}&\bar{1}&\bar{1}\\ \bar{0}&\bar{1}&\bar{1}&\bar{0}&\bar{0}&\bar{1}&\bar{1}\\ \bar{1}&\bar{0}&\bar{1}&\bar{0}&\bar{1}&\bar{0}&\bar{1}\end{pmatrix}$ y el siguiente s.v. de $\mathbb{Z}_2^7$, C_H, dado por las ecuaciones implícitas:

$$C_H=\left\{\left(\overline{x_1},\ \overline{x_2},\ \cdots\ ,\overline{x_7}\right)\in\mathbb{Z}_2^7 \,/\, \begin{pmatrix}\bar{0}&\bar{0}&\bar{0}&\bar{1}&\bar{1}&\bar{1}&\bar{1}\\ \bar{0}&\bar{1}&\bar{1}&\bar{0}&\bar{0}&\bar{1}&\bar{1}\\ \bar{1}&\bar{0}&\bar{1}&\bar{0}&\bar{1}&\bar{0}&\bar{1}\end{pmatrix}\begin{pmatrix}\overline{x_1}\\ \overline{x_2}\\ \vdots\\ \overline{x_7}\end{pmatrix}=\begin{pmatrix}\bar{0}\\ \bar{0}\\ \bar{0}\end{pmatrix}\right\}.$$

C_H es un código lineal de longitud **7**, **dimC_H=4** y **$|C_H|=2^4$**. A la matriz **H** se le llama **matriz de paridad** del código lineal C_H. Este código lineal se llama Código (7,4) de Hamming donde 7 es la longitud de las palabras del código, 4 es la dimensión del código y 2^4 el número de palabras del código.

Para obtener explícitamente todas las palabras del código lineal C_H hay que resolver el sistema homogéneo dado por las ecuaciones implícitas:

$$\left(\begin{array}{ccccccc|c}\bar{0}&\bar{0}&\bar{0}&\bar{1}&\bar{1}&\bar{1}&\bar{1}&\bar{0}\\ \bar{0}&\bar{1}&\bar{1}&\bar{0}&\bar{0}&\bar{1}&\bar{1}&\bar{0}\\ \bar{1}&\bar{0}&\bar{1}&\bar{0}&\bar{1}&\bar{0}&\bar{1}&\bar{0}\end{array}\right)\sim\left(\begin{array}{ccccccc|c}\boxed{\bar{1}}&\bar{0}&\bar{1}&\bar{0}&\bar{1}&\bar{0}&\bar{1}&\bar{0}\\ \bar{0}&\boxed{\bar{1}}&\bar{1}&\bar{0}&\bar{0}&\bar{1}&\bar{1}&\bar{0}\\ \bar{0}&\bar{0}&\bar{0}&\boxed{\bar{1}}&\bar{1}&\bar{1}&\bar{1}&\bar{0}\end{array}\right)\Rightarrow\begin{cases}\overline{x_1}=-\overline{\alpha}-\overline{\gamma}-\overline{\delta}\\ \overline{x_2}=-\overline{\alpha}-\overline{\beta}-\overline{\delta}\\ \overline{x_3}=\overline{\delta}\\ \overline{x_4}=-\overline{\alpha}-\overline{\beta}-\overline{\gamma}\\ \overline{x_5}=\overline{\gamma}\\ \overline{x_6}=\overline{\beta}\\ \overline{x_7}=\overline{\alpha}\end{cases}\Rightarrow\begin{cases}\overline{x_1}=\overline{\alpha}+\overline{\gamma}+\overline{\delta}\\ \overline{x_2}=\overline{\alpha}+\overline{\beta}+\overline{\delta}\\ \overline{x_3}=\overline{\delta}\\ \overline{x_4}=\overline{\alpha}+\overline{\beta}+\overline{\gamma}\\ \overline{x_5}=\overline{\gamma}\\ \overline{x_6}=\overline{\beta}\\ \overline{x_7}=\overline{\alpha}\end{cases}$$

$$\Rightarrow\begin{pmatrix}\overline{x_1}\\ \overline{x_2}\\ \overline{x_3}\\ \overline{x_4}\\ \overline{x_5}\\ \overline{x_6}\\ \overline{x_7}\end{pmatrix}=\overline{\alpha}\begin{pmatrix}\bar{1}\\ \bar{1}\\ \bar{0}\\ \bar{1}\\ \bar{0}\\ \bar{0}\\ \bar{1}\end{pmatrix}+\overline{\beta}\begin{pmatrix}\bar{0}\\ \bar{1}\\ \bar{0}\\ \bar{1}\\ \bar{0}\\ \bar{1}\\ \bar{0}\end{pmatrix}+\overline{\gamma}\begin{pmatrix}\bar{1}\\ \bar{0}\\ \bar{0}\\ \bar{1}\\ \bar{1}\\ \bar{0}\\ \bar{0}\end{pmatrix}+\overline{\delta}\begin{pmatrix}\bar{1}\\ \bar{1}\\ \bar{1}\\ \bar{0}\\ \bar{0}\\ \bar{0}\\ \bar{0}\end{pmatrix}$$

Dando valores $\bar{0}$ y $\bar{1}$ a los parámetros $\overline{\alpha},\overline{\beta},\overline{\gamma}$ y $\overline{\delta}$, obtenemos las 2^4 palabras del código lineal C_H.

Obsevación: si tengo S un s.v. de $\mathbb{Z}_2^n$, dado por todos los vectores de S (tendrán que ser 2^k vectores y k será la dimensión de S) y quiero calcular las ecuaciones paramétricas e implícitas de S, tendré que quedarme con los vectores de S que sean l.i., es decir, tendré que quedarme con k vectores l.i. Estos vectores forman una base de S y a partir de ellos puedo calcular las ecuaciones paramétricas de S. A continuación, eliminando parámetros, obtengo las ecuaciones implícitas de S. La matriz de coeficientes del sistema homogéneo, dado por las ecuaciones implícitas de S, es una **matriz de paridad** del código lineal S.

A partir de este momento y para simplificar la notación, las clases de $\mathbb{Z}_2$ se representarán simplemente como 0, 1.

Aplicación a la teoría de la codificación

Cuando transmitimos un mensaje puede que llegue distorsionado (mensaje mezclado o con ruido). Necesitamos enviar los mensajes de forma que cuando llegue afectado de ruido se pueda detectar este ruido y volver a su forma original. Este proceso se conoce como codificación, detección y corrección de errores y decodificación.

Por ejemplo, supongamos un mensaje cuya representación digital es 1011. Codificar 1011 significa transformar la secuencia en otra secuencia binaria, para que si el mensaje se distorsiona, es decir se produce algún error en la secuencia digital que se recibe, por ejemplo se recibe 0011, pueda detectarse y corregirse el error. Un ejemplo de codificación es la **comprobación de paridad,** es un método sencillo de detección de error pero no nos sirve para corregir el error, no es un código corrector; y además, si se cambian dos dígitos no detecta el error. El método consiste en agregar un 0 o un 1, dependiendo de si el mensaje tiene una cantidad par o impar de unos. Así, 1011 se codifica 10111; ahora si esta palabra se distorsiona a 00111 se sabe que ha ocurrido un error. Otro ejemplo de codificación es enviar el mensaje repetido, así 1011 se codifica 10111011 y si se recibe 00111011 se sabe que hay un error.

Un **código binario de longitud n** es cualquier subconjunto C de $\mathbb{Z}_2^n$; a los elementos de C se les llama **palabras** del código (o **palabras código**) y cada palabra la usamos para codificar un mensaje. Se dice que se han producido k errores en una palabra (o mensaje) si se han cambiado k bits (componentes) de la palabra.

Llamamos **peso de una palabra** $a \in \mathbb{Z}_2^n$, y notamos **w(a)** al número de unos de a. Llamamos **distancia Hamming entre dos palabras** $a, b \in \mathbb{Z}_2^n$, y notamos **∂(a,b)** al número de bits en que difieren a y b. Así, w(a)= ∂(a,0) y ∂(a,b)=w(a-b)=w(a+b) (suma módulo 2). Llamamos **distancia del código C**, y la notamos **δ(C)**, a la **distancia mínima** entre palabras distintas **del código C**, es decir

$$\delta(C) = \min\{ \partial(a,b) \,/\, a,b \in C \text{ y } a \neq b \}$$

Un código C se dice que puede detectar un error, si al cambiar un bit en una palabra del código se obtiene una palabra que no es del código C. Un código C puede corregir un error si al detectarse un error en una palabra, sólo hay una palabra del código C que está a distancia uno de la palabra con error. Un código C con distancia δ puede detectar δ-1 errores y puede corregir ***e*** errores con $\delta \geq 2\boldsymbol{e}+1$. Por ejemplo, si δ, la distancia mínima entre las palabras de C, es 3 se podrán detectar hasta dos errores y corregir un error. Si δ es 2 no se podrá corregir ningún error, será un código detector de un error pero no corrector.

Un código C en $\mathbb{Z}_2^n$ es **lineal** si C es un subespacio vectorial de $\mathbb{Z}_2^n$. Si C es un código lineal entonces δ(C) es el peso mínimo de las palabras no nulas de C, es decir

$$\delta(C) = \min\{ w(a) \,/\, a \in C \text{ y } a \neq 0 \} = w_{min}$$

Construcción de códigos lineales

Dada H una matriz binaria de *n* columnas, el conjunto C definido por

$$C = \left\{ (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_2^n \;/\; H \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \vec{0} \right\}$$

es un s.v. de $\mathbb{Z}_2^n$ y por tanto, es un código lineal de longitud *n*. La matriz H se llama **matriz de paridad** del código C, y resolviendo el sistema homogéneo $H\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \vec{0}$ obtendremos todas las palabras del código C determinado por la matriz de paridad H. Por tanto, el código C tiene dimensión n-rg(H) y el número de palabras del código es $|C|=2^{n-rg(H)}$.

Códigos lineales capaces de corregir un error

Teorema: Dada una matriz de paridad H, el código C definido por la matriz H es capaz de corregir un error si y sólo si H no contiene ninguna columna de ceros, ni dos columnas iguales.

Ejemplo: la matriz $H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ del código (7,4) de Hamming cumple las condiciones del teorema y, por tanto, es un código capaz de corregir un error. Sin embargo, la matriz $H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ no cumple el teorema ya que, tiene la primera y tercera columnas iguales, y no va a ser un código corrector. La palabra (1,0,1,0,0,0,0) pertenece al código y su distancia al origen es dos, así, la distancia del código es menor o igual a 2 y por tanto, no es un código corrector.

El método que se utiliza para detectar y corregir un solo error en un código C, que cumple las condiciones del teorema anterior, es el siguiente: sea una matriz H, de n columnas, la matriz de paridad de un código C en las condiciones del teorema anterior; sea $\vec{y} \in \mathbb{Z}_2^n$ la palabra recibida de la cual se sabe que o es una palabra del código o se ha cometido un solo error.

1. Si $H\vec{y} = \vec{0}$ entonces $\vec{y} \in C$, y por tanto no se ha producido ningún error; luego $\vec{y}$ es el mensaje enviado.
2. Si $H\vec{y} \neq \vec{0}$ entonces $\vec{y} \notin C$, y por tanto se habrá producido un error en la componente i-ésima de $\vec{y}$; luego $\vec{y} = \vec{y'} + \vec{e_i}$ con $\vec{y'}$ una palabra código. Por tanto, $H\vec{y} = H\vec{y'} + H\vec{e_i} = \vec{0} + h_i$ siendo h_i la columna i-ésima de H. Luego, si al calcular $H\vec{y}$ obtenemos la columna i-ésima de H significa que se ha producido un error en la componente i-ésima de la palabra original. Así, cambiando el bit i-ésimo de $\vec{y}$, es decir, haciendo $\vec{y} + \vec{e_i}$ obtendremos el mensaje enviado.

Observación: recordamos que la **base usual o canónica** de $\mathbb{Z}_2^n$ es,

$$B_u^{\mathbb{Z}_2^n} = \left\{ \vec{e_1} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \vec{e_2} = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \vec{e_n} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \right\}$$

Bibliografía: *Matemática Discreta*. Autor: Norman L. Biggs. Editorial: Vicens Vives.
Matemáticas Discretas. Autor: T. Veerarajan. Editorial: Mc Graw Hill.
Álgebra Lineal con Aplicaciones. Autores: George Nakos, David Joyner. Ed.: I. Thomson.

EJERCICIOS SOBRE TEORÍA DE CÓDIGOS

1) Demostrar si los siguientes códigos binarios en $\mathbb{Z}_2^4$ son lineales. Determinar en cada caso la distancia δ del código, el número de errores que pueden ser detectados y el que pueden ser corregidos
   a) C_1 = {(0,0,0,0), (1,1,0,1)}.
   b) C_2 = {(1,1,0,1), (1,0,1,1) }.
   c) C_3 = {(0,0,0,0), (1,0,1,1), (0,1,0,1), (1,1,1,1)}.
   d) C_4 = {(0,0,0,0), (1,1,1,0), (1,0,1,1), (0,1,0,1)}.

2) Resolver los Ejercicios 2, 4 y 5 de "**Espacios vectoriales generales**" de la hoja de espacios vectoriales. En cada uno de estos ejercicios encontrar una matriz de paridad del código lineal correspondiente.

3) Dado el código lineal C = {(0,0,0,0,0,0), (1,1,1,1,0,0), (0,1,1,0,1,0), (0,0,1,1,1,1), (1,0,1,0,0,1), (1,0,0,1,1,0), (1,1,0,0,1,1), (0,1,0,1,0,1)}, obtener una matriz de paridad para este código. ¿Cuál es el número de errores que detecta?, ¿y que corrige?

4) Hallar todas las palabras del código C cuya matriz de paridad es $\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$ ¿Cuál es la longitud del código C? ¿Cuál es la dimensión de C? ¿Cuál es la distancia de C?

5) Queremos ser capaces de enviar 128 mensajes diferentes y cada mensaje ha de representarse como una palabra binaria de longitud 11. Construir una matriz de paridad cuyo código asociado cumpla estos requisitos y además pueda corregir un error.

6) En la clase de Álgebra Lineal se quiere asignar un número de identidad, en forma de palabra binaria, a cada estudiante.
   a) Si hay 83 estudiantes, hallar la **dimensión mínima** de un código lineal para este propósito.
   b) Si el código lineal, para los 83 estudiantes, ha de permitir la **detección de un error**, construir las ecuaciones paramétricas e implícitas de uno de estos códigos con **longitud** de las palabras la **mínima** posible.
   c) Hallar la matriz de paridad de un código lineal de longitud 11 con el propósito del enunciado (codificar 83 estudiantes con la mínima dimensión posible) y tal que permita la **corrección** de un error. ¿Se podría hacer con longitud 9?

7) Dado un código (7,4) de Hamming y recibidos los siguientes mensajes en los que se supone que hay como máximo un error, detectar si hay error y, en su caso, corregidlo dando el mensaje original.

   a) (0,1,0,0,1,0,1) b) (1,0,0,1,0,0,1) c) (1,1,0,1,1,0,1)

8) Construir una matriz de paridad para un código de longitud 15 y dimensión 11 capaz de corregir un error. Dado el código lineal cuya matriz de paridad se ha obtenido y recibidos los siguientes mensajes en los que se supone que hay como máximo un error, detectar si hay error y, en su caso, corregirlo dando el mensaje original.

m1) (1,1,1,0,1,0,0,1,1,0,1,0,1,0,0) m2) (0,0,0,1,1,1,1,0,0,0,1,0,0,0,1) m3) (1,0,0,1,1,0,1,1,0,0,0,0,0,1,1)